### Shilpi Goel

Introduction EDCs

Formalization

Soundness Completeness Strength

Analysis CRCs

Summary

# A Formal Analysis of Error Detecting Codes Using ACL2

### Shilpi Goel

shigoel@cs.utexas.edu

The University of Texas at Austin

◆□▶ ◆□▶ ▲□▶ ▲□▶ □ のQ@

### Detecting Codes Shilpi Goel

Error

# EDCs

Formalization

Soundness Completeness Strength

Analysis CRCs

Summary

### Introduction

Error Detecting Codes What Does The Analysis Of EDCs Involve?

### Formalization

Soundness Completeness Strength



2

Analysis Of Some EDCs Analysis of CRCs



Summary

◆□▶ ◆□▶ ▲□▶ ▲□▶ □ のQ@

### Detecting Codes Shilpi Goel

Error

### Introduction

### Introduction

What Does The Analysis Of EDCs Involve?

Analysis of CRCs

◆□▶ ◆□▶ ▲□▶ ▲□▶ □ のQ@

# Shilpi Goel

Error Detecting

Codes

### Introductio

EDCs Analysis?

### Formalization

Soundness Completeness Strength

Analysis CRCs

Summary

### Introduction Error Detecting Codes

What Does The Analysis Of EDCs Involve?

### Formalization

Soundness Completeness Strength

3

Analysis Of Some EDCs Analysis of CRCs

4 Summary

### Shilpi Goel

#### Introduction

EDCs Analysis?

#### Formalization

Soundness Completeness Strength

Analysis CRCs

Summary

# **Error Detecting Codes**

▲ロ▶ ▲□▶ ▲□▶ ▲□▶ □ のQ@

• Error Detecting Codes (EDCs) detect errors that may be introduced when data is received at the destination from the source.

# Terminology

▲ロ▶ ▲□▶ ▲□▶ ▲□▶ □ のQ@

#### Introduction

Error Detecting

Codes Shilpi Goel

#### EDCs Analysis?

#### Formalization

- Soundness Completeness Strength
- Analysis CRCs
- Summary

- Sender where the data is augmented with a computed tag (converted into a codeword)
- Receiver where it is checked whether the received message is a legal codeword or not

◆□▶ ◆□▶ ▲□▶ ▲□▶ □ のQ@

### Detecting Codes Shilpi Goel

Error

### EDCs Analysis?

#### Formalization

Soundness Completeness Strength

Analysis CRCs

Summary

### Introduction

Error Detecting Codes What Does The Analysis Of EDCs Involve?

### Formalization

Soundness Completeness Strength

3

Analysis Of Some EDCs Analysis of CRCs

4 Summary

### Shilpi Goel

Introduction EDCs Analysis?

#### Formalization

Soundness Completeness Strength

Analysis CRCs

Summary

# Why Do We Need To Analyze EDCs using ACL2?

- Need to trust their correctness and know their limitations
- Come up with a general framework that can be used for proofs of the properties of all EDCs

▲ロ▶ ▲□▶ ▲□▶ ▲□▶ □ のQ@

Shilpi Goel

Introduction EDCs Analysis?

#### Formalization

Soundness Completeness Strength

Analysis CRCs

Summary

# What Does The Analysis Of EDCs Involve?

- Receiver's Point of View: the receiver's concern is to correctly detect whether the received codeword is legal or not.
- Analyzer's Point of View: the analyzer's concern is to determine what kinds of errors the EDC scheme can detect.

Shilpi Goel

Introduction EDCs Analysis?

#### Formalization

Soundness Completeness Strength

Analysis CRCs

Summary

# What Does The Analysis Of EDCs Involve?

- Soundness (Receiver's Point of View)
- Completeness (Receiver's Point of View)
- Strength (Analyzer's Point of View)

### Soundness

▲□▶▲□▶▲□▶▲□▶ □ のQ@

### Codes Shilpi Goel

Error Detecting

#### Introduction EDCs Analysis?

#### Formalization

Soundness Completeness Strength

Analysis CRCs

Summary

An informal description of soundness of an EDC:

- Given an uncorrupted transmission of data, the error control scheme ought to be able to report that the received data is error-free.
- No Error Detected ⇒ Received Codeword is Legal

## Completeness

▲□▶▲□▶▲□▶▲□▶ □ のQ@

### Codes Shilpi Goel

Error Detecting

#### Introduction EDCs Analysis?

#### Formalization

Soundness Completeness Strength

Analysis CRCs

Summary

An informal description of completeness of an EDC:

- Given a corrupted transmission of data, the error control scheme ought to be able to report that the data is corrupted.
- Error Detected ⇒ Received Codeword is Not Legal

### Shilpi Goel

Introduction EDCs Analysis?

#### Formalization

Soundness Completeness Strength

Analysis CRCs

Summary

# More About Soundness

- Merely knowing that the received codeword is legal is not enough to guarantee that the transmission was error-free.
- We need to analyze the strengths and limitations of the EDC to state under *what* conditions can we know absolutely that the transmission was error-free when it is reported as error-free.

### Strength

▲□▶▲□▶▲□▶▲□▶ □ のQ@

### Introduction EDCs Analysis?

Error Detecting

Codes Shilpi Goel

#### Formalization

Soundness Completeness Strength

Analysis CRCs

Summary

Informally, determining the strength of an EDC involves the specification of:

- The types of errors that the EDC can always detect
- Includes the analysis of the general robustness of the EDC like detecting burst errors or more specific analysis like detection of isolated two bit errors, etc

◆□▶ ◆□▶ ▲□▶ ▲□▶ □ のQ@

### Error Detecting Codes

### Shilpi Goel

### Formalization

What Does The Analysis Of EDCs Involve?

#### 2 Formalization

Analysis of CRCs

### Formalization

▲ロ▶ ▲□▶ ▲□▶ ▲□▶ □ のQ@

#### Introduction EDCs Analysis?

### Formalization

Soundness Completeness Strength

Analysis CRCs

Summary

In this section, we will formalize the concepts of soundness, completeness and strength of an error detecting scheme.

### Notation Used

◆□▶ ◆□▶ ◆臣▶ ◆臣▶ 臣 のへぐ

### Error Detecting Codes

### Shilpi Goel

### Introduction

Analysis?

### Formalization

Soundness Completeness Strength

Analysis CRCs

Summary

Term	Description
Det	predicate that detects whether the received message is a
	codeword
E	function that encodes a message
D	function that decodes a message
Env	the predicate which specifies under what environment the
	EDC works

### Error Detecting Codes

### Shilpi Goel

Soundness

What Does The Analysis Of EDCs Involve?

### Formalization Soundness

2

Analysis of CRCs



### Shilpi Goel

### Introductio EDCs

### Formalization

### Soundness

Completenes Strength

Analysis CRCs

Summary

## Soundness

▲ロ▶ ▲□▶ ▲□▶ ▲□▶ □ のQ@

Let n be the number of bits in the data the sender encodes and m be the message received by the receiver.

If Env(n,m) holds and Det(m) is false, then there exists an m' such that D(m) = m' and E(m') = m.

◆□▶ ◆□▶ ▲□▶ ▲□▶ □ のQ@

### Detecting Codes Shilpi Goel

Error

EDCs Analysis?

Formalization

Soundness Completeness

Strength

Analysis CRCs

Summary

### Introduction

Error Detecting Codes What Does The Analysis Of EDCs Involve?

### Formalization

2

Soundness

### Completeness

Strength

3 Analysis Of Some EDC Analysis of CRCs

4 Summary

### Completeness

▲□▶▲□▶▲□▶▲□▶ □ のQ@

### EDCs Analysis?

Error Detecting

Codes Shilpi Goel

#### Formalization

#### Soundness Completeness

. Strength

Analysis CRCs

Summary

Let n be the number of bits in the data the sender encodes and m be the message received by the receiver.

If Env(n,m) holds and if Det(m) is true, then there exists no m' such that D(m) = m' and E(m') = m.

### Detecting Codes Shilpi Goel

Error

### EDCs Analysis?

Formalization

Soundness Completeness Strength

Analysis CRCs

Summary

### Introduction

Error Detecting Codes What Does The Analysis Of EDCs Involve?

### 2 Formalization

Soundness Completeness Strength

3

Analysis Of Some EDCs Analysis of CRCs

4 Summary

▲□▶ ▲□▶ ▲□▶ ▲□▶ ▲□ ● のへで

### Strength

▲□▶▲□▶▲□▶▲□▶ □ のQ@

### Introduction EDCs Analysis?

Error Detecting

Codes Shilpi Goel

### Formalization

Soundness Completeness

Strength

Analysis CRCs

Summary

Let s be the encoded message sent by the sender and r be the message received by the receiver such that r is not equal to s. Errors(s,r) specifies the transformations s undergoes to become r such that r is not another legal codeword.

If Errors(s,r) holds, then Det(r) will be true.

◆□▶ ◆□▶ ▲□▶ ▲□▶ □ のQ@

### Detecting Codes Shilpi Goel

Error

Analysis CBCs



3 Analysis Of Some EDCs

### Shilpi Goel

# EDCs

### Formalization

Soundness Completeness Strength

Analysis CRCs

Summary

# Analysis of Some EDCs

- To arrive at a general framework for EDC analysis, one must examine some specific EDCs.
  - Even Parity Check
  - Weighted Checksum
  - Cyclic Redundancy Check (CRC)
- In particular, we will look at the Soundness and Completenss of Cyclic Redundancy Checks.

▲□▶▲□▶▲□▶▲□▶ □ のQ@

◆□▶ ◆□▶ ▲□▶ ▲□▶ □ のQ@

### Detecting Codes Shilpi Goel

Error

### EDCs Analysis?

Formalization

Soundness Completeness Strength

Analysis CRCs

Summary

### Introduction

Error Detecting Codes What Does The Analysis Of EDCs Involve?

### Formalization

Soundness Completeness Strength



Analysis Of Some EDCs Analysis of CRCs

4 Summar

### **CRCs**

▲ロ▶ ▲□▶ ▲□▶ ▲□▶ □ のQ@

### Introduction EDCs

Error Detecting

Codes Shilpi Goel

### Analysis?

### Formalization

Soundness Completeness Strength

### Analysis CRCs

Summary

- CRCs are cyclic linear codes based on division in the ring of polynomials over GF(2).
- CRC division, like ordinary long division, can be done by shifts and subtraction (over GF(2)).

### Shilpi Goel

### Introduction EDCs Analysis?

### Formalization

Soundness Completeness Strength

### Analysis CRCs

### Summary

### Addition/Subtraction: XOR Operation

+	1	0					
1	0	1					
0	1	0					

Multiplication: AND Operation

*	1	0
1	1	0
0	0	0

# GF(2)

(ロ)、

### EDCs Analysis?

### Formalization

Soundness Completeness Strength

### Analysis CRCs

Summary

For CRCs to work, the sender and receiver agree on:

- the generator polynomial gp, which is the divisor in the GF(2) division process
- the augment a the length of a is one less than the length of gp. a is augmented to the message at the sender's end
- the number of bits n of the message to be encoded at a time by the sender and hence, also the number of bits of the received message to be decoded at a time by the receiver

EDCs Analysis?

Formalization

Soundness Completeness Strength

Analysis CRCs

Summary

For CRCs to work, the sender and receiver agree on:

- the generator polynomial gp, which is the divisor in the GF(2) division process
- the augment a the length of a is one less than the length of gp. a is augmented to the message at the sender's end
- the number of bits n of the message to be encoded at a time by the sender - and hence, also the number of bits of the received message to be decoded at a time by the receiver

EDCs Analysis?

Formalization

Soundness Completeness Strength

Analysis CRCs

Summary

For CRCs to work, the sender and receiver agree on:

- the generator polynomial gp, which is the divisor in the GF(2) division process
- the augment a the length of a is one less than the length of gp. a is augmented to the message at the sender's end
- the number of bits n of the message to be encoded at a time by the sender and hence, also the number of bits of the received message to be decoded at a time by the receiver

### Shilpi Goel

### EDCs Analysis?

#### Formalization

Soundness Completeness Strength

Analysis CRCs

Summary

### An Example

### Let gp be 101 and m' be 1001. Hence, n is 4.

a should be of length 2.

Let a be 11.

・ロト・(四ト・(日下・(日下・))への)

### Shilpi Goel

#### Introduction EDCs Analysis?

### Formalization

Soundness Completeness Strength

Analysis CRCs

Summary

### An Example

### Let gp be 101 and m' be 1001. Hence, n is 4.

a should be of length 2.

Let a be 11.

◆□ → ◆□ → ◆三 → ◆三 → ● ◆ ● ◆ ●

### Shilpi Goel

#### Introduction EDCs Analysis?

### Formalization

Soundness Completeness Strength

### Analysis CRCs

Summary

### An Example

### Let gp be 101 and m' be 1001. Hence, n is 4.

a should be of length 2.

Let a be 11.



Error Detecting Codes	Sender's End
Shilpi Goel Introduction EDCs Analysis?	$gp = 1 \ 0 \ 1$ m' = 1 \ 0 \ 0 \ 1 a = 1 \ 1
Formalization Soundness Completeness Strength	<b>1 0 1</b> ) <b>1 0 0 1 1 1</b> ( 1 0 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
Analysis cRcs Summary	
	00 is the computed tag (or CRC).

Error Detecting Codes								Se	end	er	's E	nd	
Shilpi Goel		<u>e</u> =											
Introduction EDCs Analysis?				) 1									
Formalization Soundness Completeness Strength	1					1	1						
Analysis CRCs													
Summary													

00 is the computed tag (or CRC).

・ロト・四ト・モート ヨー うへの

# Error Sender's End Detecting Codes Shilpi Goel qp = 101m' = 1001Analysis? Strength Analysis CRCs ▲□▶ ▲□▶ ▲□▶ ▲□▶ = 三 のへで

# Error Sender's End Detecting Codes Shilpi Goel gp = 101m' = 1001**a** = 11 Analysis? Strength Analysis CRCs

◆□▶ ◆□▶ ◆臣▶ ◆臣▶ ─臣 ─のへで

Error Detecting Codes	Sender's End
Shilpi Goel Introduction EDCs Analysis?	$\begin{array}{l} \mathbf{gp} = 1 \ 0 \ 1 \\ \mathbf{m'} = 1 \ 0 \ 0 \ 1 \\ \mathbf{a} = 1 \ 1 \end{array}$
Formalization Soundness Completeness Strength	<b>1 0 1</b> ) <b>1 0 0 1 1 1</b> ( 1 0 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
Analysis crcs Summary	0 1 1 1 1 0 0 0 
	1 0 1 1 0 1 
	00 is the computed tag (or CRC). 《마》《문》《書》《書》《書》》 홈 -

### Error Sender's End Detecting Codes Shilpi Goel qp = 101m' = 1001**a** = 11 **101)100111**(1011 1 0 1 Strength \_\_\_\_\_ CRCs 0 1 1 1 1 0 0 0 \_\_\_\_\_ 1 1 1 1 1 0 1 \_\_\_\_\_ 1 0 1 1 0 1 \_\_\_\_\_ 0 0 00 is the computed tag (or CRC). ◆□▶ ◆□▶ ◆臣▶ ◆臣▶ ─臣 ─のへで

Error Detecting Codes Shilpi Goel					
EDCs Analysis?					
Formalization Soundness Completeness Strength	1				
Analysis cRcs Summary					

## **Receiver's End**

## **Uncorrupted Transmission**

11 is the computed tag (or CRC)

# Error Detecting Codes Shilpi Goel 1 0 Strength Analysis CRCs

## **Receiver's End**

### **Uncorrupted Transmission**

1

0	1	)	<b>0</b> 0		1	0	0	(	1	0	1
				1 0	1 0	0	0				
			 		1 0		0				
			 			1 0					
			 			1	1	-			

**11** is the computed tag (or CRC)

▲□▶ ▲□▶ ▲□▶ ▲□▶ ▲□ ● のへぐ

# Error Detecting Codes Shilpi Goel Analysis? Strength Analysis CRCs

## **Receiver's End**

## **Uncorrupted Transmission**

1	0	1	)	<b>0</b> 0		1	0	0	(	1	0	1	1
					1 0		0	0					
				 		1 0	0 1	0	-				
				 			1 0		-				
				 			1	1	-				

**11** is the computed tag (or CRC).

▲□▶ ▲□▶ ▲□▶ ▲□▶ ▲□ ● のへぐ

### EDCs Analysis?

F						

Soundness Completeness Strength

Analysis CRCs

Summary

## **Receiver's End**

## **Corrupted Transmission**

Instead of 1 0 0 1 0 0, the receiver receives 1 1 0 1 0 0.

1							

1 0 is not equal to a.

▲□▶ ▲□▶ ▲□▶ ▲□▶ ▲□ ● のへぐ

Error Detecting Codes Shilpi Goel

EDCs Analysis?

Soundness Completeness Strenath

Analysis CRCs

Summary

## **Receiver's End**

**Corrupted Transmission** 

Instead of  $1 \ 0 \ 0 \ 1 \ 0 \ 0$ , the receiver receives  $1 \ 1 \ 0 \ 1 \ 0 \ 0$ .

**101**) 110100 (1110 1 0 1 \_\_\_\_\_ 1 1 1 0 0 1 0 1 \_\_\_\_\_ 0 0 1 0 1 0 1 \_\_\_\_\_ 0 1 0 0 0 0 \_\_\_\_\_ 1 0

1 0 is not equal to a.

▲□▶▲□▶▲□▶▲□▶ □ のQ@

Error Detecting Codes Shilpi Goel

EDCs Analysis?

Soundness Completeness

Strength Analysis CRCs

Summary

## **Receiver's End**

**Corrupted Transmission** 

Instead of  $1 \ 0 \ 0 \ 1 \ 0 \ 0$ , the receiver receives  $1 \ 1 \ 0 \ 1 \ 0 \ 0$ .

**101**) 110100 (1110 1 0 1 \_\_\_\_\_ 1 1 1 0 0 1 0 1 \_\_\_\_\_ 1 0 0 0 1 0 1 \_\_\_\_\_ 0 1 0 0 0 0 \_\_\_\_\_ 1 0

1 0 is not equal to a.

▲□▶▲□▶▲□▶▲□▶ □ のQ@

### Error Detecting Codes

### Shilpi Goel

#### Introduction

EDCs Analysis?

#### Formalization

Soundness Completeness Strength

### Analysis CRCs

Summary

## ACL2 Definitions

◆□▶ ◆□▶ ▲□▶ ▲□▶ □ のQ@

## The Environment Predicate:

```
(defun Env (n m a gp)
 (and (<= 1 (len gp))
      (natp n)
      (< 0 n)
      (equal (car gp) 'T)
      (equal (len m) (+ n (len a)))
      (equal (len a) (1- (len gp)))
      (boolean-listp gp)
      (boolean-listp m)
      (boolean-listp a)))
```

### Error Detecting Codes

### Shilpi Goel

## EDCs Analysis?

## Completeness Strength

### Analysis CRCs

```
Summary
```

## ACL2 Definitions

## The Detecting Predicate:

```
(defun Det (m a gp)
  (not (equal (crc m gp) a)))
```

## Encoding Function:

## **Decoding Function:**

```
(defun D (m gp)
(firstn (- (len m) (1- (len gp)))
m))
```

### ・ロト・西ト・ヨト・ヨー シック・

## Soundness

▲□▶▲□▶▲□▶▲□▶ □ のQ@

## EDCs

Error Detecting

Codes Shilpi Goel

#### Formalization

Soundness Completeness Strength

### Analysis CRCs

Summary

## Completeness

¢	completeness-crc
]	lies (and (Env n m a
	(Det mag

Error Detecting

Codes Shilpi Goel

> (Det m a gp)) (not (exists-D-E m a gp))))

### Error Detecting Codes

### Shilpi Goel

#### Introduction EDCs Analysis?

#### Formalization

Soundness Completeness Strength

### Analysis CRCs

Summary

## Strength Of CRCs - Work In Progress

```
(defun burst-error (s r gp)
 (< (len (strip-nils-at-ends (bv-xor s r))) (len gp)))</pre>
```

```
(defthm strength-of-crc
(implies (and (Env n r a gp)
                (equal s (E m- a gp))
                     (boolean-listp m-)
                     (equal (len m-) n)
                     (equal (car (last gp)) 'T)
                     (burst-error s r gp))
                     (Det r a gp))))
```

## Outline

### Detecting Codes Shilpi Goel

Error

### EDCs Analysis?

Formalization

Soundness Completeness Strength

Analysis CRCs

Summary

### Introduction

Error Detecting Codes What Does The Analysis Of EDCs Involve?

### Formalization

Soundness Completeness Strength



Analysis Of Some EDCs Analysis of CRCs



Summary



## Summary

◆□▶ ◆□▶ ▲□▶ ▲□▶ □ のQ@

#### Introduction EDCs Analysis?

Error Detecting

Codes Shilpi Goel

#### Formalization

Soundness Completeness Strength

Analysis CRCs

Summary

- As of now, we have done a formal analysis of soundness, completeness and strengths of some EDCs.
- We aim to arrive at a general framework to prove the correctness and strengths of all EDCs.
- Doing a similar analysis for Error Correcting Codes would be interesting too.